

REMARKS

Reconsideration and allowance of the above referenced application are respectfully requested.

Initially, applicants apologize for the failure to previously amend Claim 21. This amendment is made herein and should obviate the objection thereto.

Claim 9 stands rejected under 35 USC 112, first paragraph, as allegedly failing to comply with the enablement requirement. The objection is made that there is no description or example of cards optimized for encryption of SONET or ATM. Initially, applicants note that page 9, fourth line from the bottom, specifically states that "the hardware unit is optimized for the specific function, here encrypting SONET/SDH, and may produce very high throughput for that particular operation". The rejection, and the response to arguments, appears to contend that there is no description of how to optimize for encrypting SONET or SDH. However, it is respectfully suggested that this standard is legally incorrect. A patent need not disclose, and in fact preferably omits, that which is known in the art. Those having ordinary skill in the art understand that different hardware can be optimized for different kinds of encryption. For example, and as explained in paragraph 25 at the top of page 10, specialized equipment can be used for the different functions.

Applicants did not mean that this was optimized, in the sense that it was the absolute best one that had ever been created. Rather, applicants mean that the card is specialized for different functions.

In order to obviate that interpretation, the term "optimized" has been changed to "specialized". It is admitted that those having ordinary skill in the art certainly understand that one piece of hardware could be specialized for ATM, another specialized for SONET. This does not require optimization, and in fact the top of page 3 goes so far as to call this "trivial to a person skilled in encryption of data packet". While this may be trivial, it certainly could increase the throughput.

For these reasons, it is respectfully suggested that Claim 9 should be in condition for allowance.

Claim 10 stands rejected under 35 USC 112, first paragraph, as allegedly failing to comply with the enablement requirement. Again, applicants respectfully suggest that the mere discussion of the security interlock with a memory erased function would teach a person of ordinary skill in the art how to do this. Initially, applicants apologize for the typographical error which referred to Claim 22 instead of paragraph 22. However, paragraph 22 describes that when power is removed, the keys are destroyed. Page 3 of the official action states that these describe what should happen, but provides no enablement how to

do it. This function, however, is clearly within the understanding of those having ordinary skill in the art. The rejection itself cites U.S. patent number 6,426,706 ("King"). In item 11.1 of this rejection, the patent office states that King "also teaches a memory erasure function that erases memory upon receiving a violation warning". Since the patent office contends that King shows how to erase memory, it is clear that this provides evidence that the erasure of memory is well-known in the art. Also, as described in the previous amendment, there were 678 patents that showed how to provide a level to an EEPROM that caused its erasure. The previous amendment described U.S. patent number 7,099,220 as evidence that shows that those having ordinary skill in the art would well understand how to erase a memory. Since Section 4.2 agrees that the cited paragraphs describe what should happen, and at least 7,099,220 explains how to erase the memory, that this rejection is incorrect.

Claims 1-8 and 11-23 stand rejected under 35 USC 102 as allegedly being unpatentable over Minear et al. This contention has been obviated by the amendment of Claim 1 herein to recite that a high speed crypto system includes dedicated hardware for a first format and second dedicated hardware for a second format. This is described in the middle of page 9 of the specification.

Initially, applicants have reviewed Section 4.3 of this official action and agree in retrospect that firewall must connect between a protected network and an unprotected network. However, Claim 1 is now amended, and as amended, recites a number of different elements. Basically, the point of Claim 1 is to provide a number of different optimized and unoptimized encryption and decryption structures, that can be used for different items. Claim 1, defines first and second high speed crypto systems. These two crypto systems are used for different formats of messages. Since one crypto system is used for one format and another for another format, these formats of cryptosystems can be very quickly handled in this hardware. Minear et al. does not disclose this claimed subject matter of first and second high speed crypto systems, which use dedicated hardware components for cryptographic encryption of a special format.

In addition, however, Claim 1 defines that there is a second lower speed crypto system that carries out the cryptographic operations without dedicated hardware. Minear et al. discloses a software and hardware encryption part. However, Claim 1 is also amended to recite that the lower speed crypto system also carries out at least one function other than encryption and decryption. Minear et al. does not disclose that

subject matter, and therefore, this forms one additional reason for patentability of Claim 1.

The dependent claims which depend from Claim 1 should be allowable for analogous reasons.

Claim 2 requires FPGAs. This is not disclosed by Minear et al. On page 4 of the official action, the rejection states that no specific advantage of FPGAs is disclosed by the specification or Claim 2. While this may be true, the advantages of an FPGA are inherent. The statement that FPGAs "are simply a design choice to implement a hardware firewall" may be appropriate for a rejection under 35 USC 103. However, the rejection of Claim 2 was under section 102. Since FPGAs are not identically disclosed by Minear et al., with all due respect, the rejection of Claim 2 is inappropriate. Even if the Microsoft document states that FPGAs are "commonly used to develop hardware modules", there is no disclosure that FPGAs have been commonly used to develop crypto modules that are configured to carry out a specific encryption or decryption operation. The advantages of this are inherent: that the FPGAs can be reconfigured to carry out different crypto graphic functions, e.g. for different kinds of encryption. Nowhere is there any disclosure of this, or any suggestion of this, in the prior art.

Claim 4 requires a key management subsystem that communicates using a network management protocol. While Minear

et al. does teach a key management mechanism, this key management mechanism is on the firewall itself. The rejection draws attention to column 5 lines 63 to 64 which states " the key management mechanism is in place on the firewall". Since the key management mechanism is "on the firewall" there would be no need to communicate with it via a network interface or network management protocol.

The rejection also draws attention to column 7 lines 22-37. This states that the private keys are stored in a table, and that access to that table is limited. Again, this does not teach anything about the network management protocol used for a separate key management subsystem.

In order to emphasize these advantages, however, Claim 4 is amended to recite that the key management subsystem is physically separate from the processing part.

Claim 5 defines SNMP, and while SNMP may be conventional to manage communication over a network, as shown above, the keys are not managed over a network. Rather, the keys are local to the firewall 350. Therefore, Claim 5 should be further allowable.

Claim 7 defines that the key management system maintains addresses of other management systems. While Minear et al. clearly does maintain certain addresses, there is no disclosure

in Minear et al. that it maintains the addresses of other key management systems.

Claim 11 defines a cryptographic header that is used to replace the header in the message.

Minear et al. teaches using an IPsec header to encapsulate the packets into and between the two devices. This encryption encapsulates an existing packet inside a larger packet.

Claim 11, however, requires that the header is removed and replaced with the cryptographic header. Minear et al. does not replace the header, but rather encapsulates it. Since the header is still there in Minear et al., it is not "removed" or "replaced". In the response to arguments, the patent office correctly points out that Claim 11 does not specify that the packet length is changed. However, Claim 11 does require that the header is removed and replaced. Since the header in Minear et al. is simply encapsulated, it is never removed, and hence is never removed and replaced. Accordingly, Claim 11 should be additionally allowable for these reasons.

Claims 12-21 are stated to be "substantially the same" as Claims 1 through 11. While this contention is respectfully traversed, it is respectfully suggested that these claims should be allowable for their own reasons.

Claim 12 has been amended to recite that the key management subsystem is physically separate from the processing part and

communicates via a network protocol. This should be allowable for reasons discussed above.

Claim 13 defines that the network protocol is SNMPV3, which is nowhere suggested by Minear et al., and should be allowable as discussed above.

Claim 18 has been amended to include similar limitations to those added to claim 1, and should be allowable for similar reasons to those discussed above with respect to Claim 1.

Many of the dependent claims should be similarly allowable for reasons discussed above.

For example, Claim 21 defines that the encryption and decryption system removes the header associated with the network protocol and then regenerates the header. As discussed above, Minear et al. simply encapsulates the entire message, and does not remove the header.

Claim 22 defines encrypting data, and storing and managing at least one signing key in a separate unit from the unit to carry out the encryption. This is a completely new concept, and one that is nowhere disclosed or suggested by Minear et al. As described above, Minear et al. specifically states that the keys are located in the firewall. The cited section of Minear et al., column 10 lines 30-52, describes a concept called network separation which divides a system into independent regions, each with a domain and protocol stack. Each of the protocol stacks

has its own independent set of data structures etc. A proxy 50 can act as the go-between between domains. This is one technique of preventing a hacker from obtaining control of the entire network. However, Minear et al says not one word about maintaining the keys in a different portion of the network. Minear et al. says not one word about storing and managing the signing key in a separate unit from the unit carrying out the encryption. In fact, presumably even when the figure 4 embodiment of Minear et al. were used, the signing key would still be maintained within the same unit that carries out the encrypting. There is certainly no disclosure to the contrary in Minear et al. Therefore, Claim 22 is clearly different than Minear et al., and hence should be allowable.

Claim 23 defines removing a header, encrypting a message fragment and regenerating the header. As disclosed previously, Minear et al. discloses encapsulating the entire message, not removing the header and replacing it as claimed.

Claims 9 and 24 stand rejected over Minear et al. in view of Gai et al. This contention is further respectfully traversed. While Gai et al. does teach applying this method to both ATM and SONET, there is no disclosure of specific cards, one specialized for ATM and the other specialized for SONET. Therefore, the hypothetical combination simply teaches a Minear et al. type system along with teaching that such systems can be

used for ATM and SONET. There is no disclosure of specialization of the type claimed.

Claim 10 stands rejected over Minear et al. in view of King. King, however, teaches a safety transceiver, and that safety transceiver does, in fact, have tamper detection circuitry. Applicants will freely admit that tamper protection circuitry is well-known in the art. However, there is no teaching, suggestion or disclosure of using tamper protection circuitry to protect cryptographic keys, either in this art or in any other art. The statement that these are analogous because they are both directed to security systems may be true. However, King only teaches that when the interlock is broken, "the safety warning transceiver may be rendered unusable". One of the ways it is by erasing data from the memory. A person reading this, however, would obtain no teaching to erase a key management system as claimed. Therefore, Claim 10 should be further allowable.

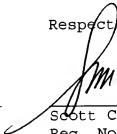
It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed.

Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Applicants asks that all claims be allowed. Please apply the \$60 extension of time fee and any credits or additional charges to deposit account 06-1050.

Respectfully submitted,

Date: March 29, 2007



Scott C. Harris
Reg. No. 32,030

Fish & Richardson P.C.
PTO Customer No. 20985
12390 El Camino Real
San Diego, California 92130
(858) 678-5070 telephone
(858) 678-5099 facsimile

10722673.doc